مجله فقه و تاریخ تمدن، دوره ۵، شماره ۱، بهار ۱۳۹۸، صفحه ۱- ۵

مسئولیت بین المللی در قبال حملات سایبری

حمیدرضا آقابابایان دامغانی[۱]، ابومحمد عسگرخانی[۲]، سید باقر میرعباسی[۳]

[۱]دانشجوی دکتری حقوق بین الملل عمومی دانشگاه آزاد واحد بین الملل قشم
[۲]دانشیار دانشکده حقوق و علوم سیاسی دانشگاه تهران
[۳]استاد دانشکده حقوق و علوم سیاسی دانشگاه تهران

نویسنده مسئول:haghababaeian@yahoo.com
تاریخ دریافت: ۱۳۹۷/۰۸/۱۶/ تاریخ پذیرش: ۱۳۹۸/۰۱/۱۷

چکیده

جنگ سایبری یابه اصطلاح دیگر نبرد مجازی به نوعی ازجنگ اطلاق می شود که درآن مستقیما ملت ها باهم درجنگ نیستند بلکه رایانه وشبکه های اینترنت یک کشور درمقابل یک یاچند کشور قرار می گیرند ودرواقع این نبرد درفضای مجازی صورت می گیرد.فضایی که شایدامروزه به جرات بتوان گفت درآن اتفاقات و حوادث زودتر ازواقعیت پیش می رود.این نوع جنگ خود شیوه نوینی درمبارزات به شمار می رود و خود مظهر نوعی دگرگونی وانقلاب درشیوه جنگ بین دولتهاست که شامل جنگ روانی ، جنگ هکرها ،جنگ اقتصادی ، جنگ و... می شود. مبارزه باحملات وجنگ سایبری درواقع نشان دهنده اقتدارکشورهاست که به چه میزانی دراین عرصه قدرت دارند واین خودنوعی مسولیت بین المللی را به وجود می آورد. نباید از یاد برد که امکان جمع آوری اطلاعات و ترتیب دادن حملات اینترنتی در فضای سایبر، توانایی وارد آوردن خسارتهای بزرگ را برای کشورهای کوچک، گروه های تروریستی و حتی افراد معمولی فراهم میآورد.درواقع استفاده ازحملات سایبری بیشترتوسط جوامع توسعه یافته علیه جوامع جهان سومی یا کمتر توسعه یافته صورت می گیرد که این مساله خود به شکلی تبعیض و تهدید جوامع جهان اولی و توسعه یافته را علیه جوامع ضعیف وجهان سوم رانشان می دهد.
کلیدواژه: فضای سایبری، مسئولیت بین المللی، شیوه نوین، مبارزات

مقدمه

همانطورکه پیداست امروزه با نوآوری درعرصه های گوناگون اطلاعاتی عصرما، عصرارتباطات و اطلاعات نامیده می شود. پس درنتیجه بااین دگرگونی ها جابه جایی اطلاعات واهمیت آن برای دولتها ازجایگاه ویژه ای برخوردار است وبا به وجود آمدن اینترنت و ماهواره و به طور کلی فضای مجازی زیرساخت های اطلاعاتی جوامع با تغییرات شگرفی مواجه شد.ولی از طرفی دیگر بابه وجود آمدن این نوع شبکه ها و ارتباطات مجازی همیشه نگرانی های بین المللی نیز روبه افزایش بود .زیرا که این خطر جوامع ضعیف تر را مورد تهدید جدی قرار می داد که جوامع غربی وپیشرفته از این نوع تکنولوژی پیشرفته برای به زیر سلطه گرفتن جوامع ضعیف تراستفاده کنند که این مساله در بحث حملات سایبری نمود پیدا کرد که خود نوعی تجاوز در مسایل اساسی یک کشور به شمار می رود که کنترل یک کشور یا دولت به صورت مفروض دراختیار دولت یاکشوری دیگر قرار می گیرد. در این راستا جامعه بین المللی شاهد حملات زیادی به اطلاعات رایانه ای در عرصه های اقتصادی، بانکی، انرژی و... بوده است.

حملات سایبری درفضای مجازی

بدون شک، همانطور که ذکر شد، یکی از پیچیده ترین ابزاری که تاکنون از آن برای اهداف تروریستی بهره برده شده است، اینترنت می باشد. تنها در دنیای اینترنت است که تروریستها می توانند با هزاران نام مجازی و بدون این که ردی از خود بر جای بگذارند، حمله ای را که ممکن است آغازگر جنگی باشد، به راه اندازند. . حمله سایبری به حمله هدایت شده از طریق فضای سایبر با توسل به ابزارها و تجهیزات سایبری را گویند. دراین راستااقتصاددانان نیز فضای سایبر را پنجمین قلمرو جنگ افروزی بعد از زمین، دریا، هوا، فضا تعریف می کنند (Law Journal of Science and Technology, Vol. 18, Issue 1 ,2008, pp. 293-324).

حمله سایبری به مثابه فعل متخلفانه بین المللی

اصول مسئولیت دولت بابت اعمال متخلفانه بین المللی ابتدائا توسط دیوان دائمی دادگستری در قضیه لوتوس بیان شد,(PCIJ, 1927, PCIJ Reports, Series A, No. 10) دیوان در این قضیه بیان داشت که حقوق بین الملل قاعده مسئولیت دولت برای نقض تعهدات وظایف بین-المللی و جبران خسارت حاصله از آن را تأیید می نماید. در حال حاضر طرح پیش نویس مسئولیت بین المللی دولت ها حاکم بر چارچوب حقوقی مسئولیت بین المللی دولت هاست (http://www.ilsa.org/jessup/jessup06/basicmats2/DASR.pdf) ماده ۳ طرح مسئولیت دولت ها به تفصیل در خصوص عناصر فعل متخلفانه بین المللی دولت صحبت کرده است. یک رفتار زمانی می تواند متخلفانه محسوب شود که نقض یک تعهد بین المللی بوده و در عین حال به دولت قابل انتساب باشد. اصطلاح نقض تعهد بین المللی پیش از این در قضیه بارسلونا تراکشن توسط دیوان بین¬المللی دادگستری بیان شده بود,(Belgium v. Spain), 1970, ICJ Reports,para. 174.

مسئولیت بین المللی دولت ها برای نقض تعهدات بین المللی از رهگذر حملات سایبری

مسئله مسئولیت دولت یکی از قدیمی ترین مسائل حقوق بین الملل است که ابتدائاً برای حمایت از بیگانگان مدنظر قرار گرفت و توسعه یافت و سپس در رابطه دولت با دولت مطرح شد. خاستگاه این اصل در رویه قضایی به رأی دیوان دائمی دادگستری در قضیه کارخانه کروزوف بر می گردد. دیوان در این قضیه اعلام کرد: یک تعهد کلی برای دولت ها وجود دارد که در برابر هر نقض تعهد جبران خسارت داشته باشند. از نظر دیوان مسئله جبران خسارت یک جزء لاینفک ناشی از رفتار خلاف یک دولت است و لذا نیازی به ذکر آن در کنوانسیون نیست(the merits), 1928 P.C.I.J. (ser.A) No. 17 (sept. 13) ,(http://www.worldcourts.com/pcij/eng/decisions/1928.09.13Corfo Channel Case, (UK V. Albania . merits,I.C.J Reports,1949,p. 37 همین موضوع در قضیه کانال کورفو نیز مورد تأیید قرار گرفت (merits,I.C.J Reports,1949,p. 37.)

حمله سایبری ومنع اصل توسل به زور

ممنوعیت توسل به زور مندرج در بند چهارم ماده ۲ منشور(متن دوزبانه منشورسازمان ملل متحد، جعفرتوانا ،) این بند مقرر می دارد: اعضای سازمان ملل متحد در روابط بین المللی خود از تهدید یا توسل به زور علیه تمامیت ارضی ، استقلال سیاسی هر کشور یا هر گونه رفتاری که با اهداف ملل متحد مطابقت ندارد، خودداری خواهند کرد. به اذعان دیوان بین المللی دادگستری در قضیه فعالیت های مسلحانه در قلمرو کنگو سنگ بنای منشور ملل متحد است (Congo v.Oganda),2005,I.C.J. Reports 2005, p. 82,para 148) با این وجود تعریف دقیق توسل به زور و این که چه اعمالی توسل به زور تلقی می¬شوند، مشخص نیست. منشور و هیچ یک از اسناد بین المللی دیگر به این مسئله نپرداخته است که این خود باعث نوعی سردرگمی می شود.وما به دنبال تسری ممنوعیت توسل به زور به فضای سایبر و حملات طراحی شده از این فضا هستیم. در این راستا دیدگاه¬های پیرامون معنای زور و هدف و مفهوم متداول طرح چنین ممنوعیتی در منشور مورد بررسی قرار می گیرد. معنای زور در بند ۴ ماده ۲ منشور ملل متحد مبنای حقوقی نوین ممنوعیت توسل به زور با ماده (۴) ۲ منشور آغاز می شود(میثاق جامعه ملل و پیمان ۱۹۲۸ بریان کلوگ بین وزرای امور خارجه ایالات متحده انگلستان و آمریکا هم متضمن اصل منع توسل به زور بودند، اما با وقوع جنگ دوم جهانی دولت ها به این نتیجه رسیدند که این اسناد برای جلوگیری از توسل به زور کافی نبوده است.) ممنوعیت توسل به زور همان گونه که دیوان دادگستری بین المللی در قضیه فعالیت های نظامی و شبه نظامی در نیکاراگوئه بیان داشته، برای اعضای سازمان ملل متحد به دلیل آمره بودن این اصل و ویژگی معاهداتی منشور الزام آور است و در عین حال برای کشورهای غیر عضو هم بر این مبنا که بیانگر قاعده عرفی حقوق بین الملل است، لازم الاجرا می باشد.(Judgment of 27 june 1986 merits, para. 174 & 188)

حمله سایبری به عنوان تجاوز یا حمله مسلحانه

حقوق بین الملل معاصر توسل به زور بین دولت ها را جز در مورد مجوز شورای امنیت و دفاع مشروع منع می کن U.N Charter .) (art.2,para.4;Arts.39&51 بنابراین نقض بند ۴ ماده ۲ عملی غیرقانونی است، این که چه اعمالی نقض بند ۴ ماده ۲ محسوب می شود و مشخص نیست و عبارت « حمله مسلحانه و تجاوز» که در منشور بیان شده، قطعاً ناقض منشور محسوب می شوند. در منشور ملل به عمل تجاوزAct of Aggression با رویکرد غیرکیفری نگریسته شده و احراز و تشخیص تجاوز به موجب ماده ۳۹ در صورت وقوع واقعه نظامی میان دو کشور یا بیشتر به عهده شورای امنیت گذاشته شده است. در سال ۱۹۷۴ مجمع عمومی قطعنامه ۳۳۱۴ را با اجماع و به منظور رفع خلاء حقوقی موجود در تعریف تجاوز تصویب نمود که هر چند فاقد ضمانت اجرایی بوده ولی به عنوان راهنما برای شورای امنیت قابل استفاده می باشد. این قطعنامه اولاً تجاوز را محدود به توسل به زور سنتی استفاده کرده و در نهایت بر مفاهیم سنتی تمامیت سرزمینی تکیه دارد http://daccess-dds (ny.un.org/doc/resolution/GEN/NRO/739/16/NRO73916.pdf) ماده ۱ قطعنامه ۳۳۱۴ در تعریف تجاوز آورده است: « بکارگیری نیروی مسلح توسط یک کشور، علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی کشور دیگر و یا کاربرد آن از سایر راه های مغایر اهداف ملل متحد (Deffinition of aggression), 1974,Art.1 قسمت آخر ماده ۱ اشاره به اشکال نظامی توسل به زور در ماده ۳ قطعنامه کرده و تمامی آن ها را تجاوز محسوب می نماید. ماده ۳ قطعنامه هم با ذکر مصادیق تعریف ماده ۱ را تکمیل می کند، آن مصادیق عبارتند از: تهاجم با ورود نیروهای ارتشی و اشغال پس از آن که خود تا هر زمان ادامه یابد، نیز ضمیمه کردن خاک یک کشور حتی بدون درگیری نظامی بمباران و فرو فرستادن موشک (بدون حضور نیروی انسانی)، محاصره

دریایی، حمله در خارج از سرزمین مثلاً به نیروهای نظامی یا ناوگان غیرنظامی دریایی و هوایی در دریا یا هوا، بیرون نرفتن نیروهای نظامی پس از ختم قرارداد از خاک یک کشور یا تعهدات آن ها در مدت قرارداد، معاونت دولت ثالث برای عبور از سرزمین او و بالاخره تجاوز غیرمستقیم از طریق اعزام نیروهای نامنظم نظامی به خاک کشور دیگر. ماده ۴ قطعنامه از تمثیلی بودن فهرست بالا صحبت کرده و اختیار تعیین سایر اعمال تجاوزکارانه را بعهده شورای امنیت نهاده است. با توجه به این که مثال های بیان شده در قطعنامه همه حکایت از اقدامات نظامی مسلحانه سنتی دارد، جای دادن حملات سایبری در بین این دسته دشوار می باشد، تأکیدات بالا من جمله تأکید بر مفاهیم سنتی تمامیت ارضی و نمونه آوردن جنگ های تجاوزی سنتی حاکی از آن است که قطعنامه، حمله به ساختارهای کلیدی یک دولت از طریق شبکه الکترونیکی آن را به عنوان تجاوز نمی شناسد، زیرا که این حملات تجاوز فیزیکی به تمامیت ارضی یک دولت با توسل به ابزارهای سنتی مسلحانه محسوب نمی شود. چنین برداشتی هماهنگ با کارهای مقدماتی در تصویب قطعنامه است که به روشنی حاکی از آن می باشد که سایر عملیات خارج از محدوده تعریف شده من جمله آن هایی که نتایج اقتصادی در پی دارد نمی تواند به عنوان عمل بین المللی تجاوز شناخته شود.(public international law systemic issues Wasrzawa 199,p.486) . نتایج زیانبار توسل به سلاح های سنتی را در پی داشته باشد می تواند دلیل قانع کننده ای برای شورای امنیت به منظور جای دادن این حملات در ماده ۳۹ منشور باشد.

حمله سایبری به عنوان حمله مسلحانه

ماده ۵۱ منشور سازمان ملل مقرر می دارد: « هیچ یک از مقررات این منشور به حق ذاتی دفاع از خود خواه به طور فردی و خواه دسته جمعی در صورت وقوع حمله مسلحانه علیه یک عضو ملل متحد تا زمانی که شورای امنیت اقدامات لازم برای حفظ صلح و امنیت بین المللی را به عمل آورد، لطمه ای وارد نخواهد کرد. بنابراین پیش شرط توسل به دفاع از خود مطابق ماده ۵۱ منشور، وقوع حمله مسلحانه است؛ مفهومی دقیق تر نسبت به توسل به زور ماده (۴) ۲ منشور(American Journal of International Law, 1985, p. 405.) .بنابراین توسل به زورهایی که حمله مسلحانه محسوب نشوند، نمی توانند موجبی برای اقدام یک جانبه دولت در راستای دفاع مشروع مطابق ماده ۵۱ منشور باشد. این عبارت مضیق بیانگر تمایل منشور به پاسخ-های جمعی در مقابل اقدامات فردی است .(Schachter, Oscar, op. cit., p. 127.) در خصوص حملات سایبری هم به واسطه مشکلاتی که دولت ها در تعیین منشا حملات خواهند داشت، این رویکرد محتاطانه تر است.

ضابطه ومیزان اثر حمله سایبری ودیدگاه حقوقدانان

سوال اینجاست که آیا هر گونه اعمال زور سایبری منجر به حمله مسلحانه می شود؟ این سوال از آن جا مطرح است که برخی متخصصان می گویند که هر گونه توسل به زور توسط نیروهای مسلح منظم یک حمله مسلحانه محسوب می شود (International Law Working Paper 05/01, Oct. 2005, available at. طبق این نظر، هر اقدام تهاجمی توسط واحد سایبری ارتش حمله مسلحانه است، زیرا که از سوی نیروهای مسلح دولت صورت گرفته است. ایالات متحده، ایران، اسرائیل و سایر دولت ها بودجه زیادی را به واحدهای ارتشی سایبری اختصاص داده اند Planck Yearbook ofUnited Nations Law 85, 97-98.) اعمال متجاوزانه توسط این واحدها ظاهراً یک حمله مسلحانه و موجد حق دفاع مشروع محسوب می شود. خطر اینجاست که یک پیغام صرف از سوی یک سرباز می تواند دولت را در یک مخاصمه طولانی گرفتار کند.(Congo v. Uganda), I.C.J Reports 2005,, P. 216 . اما این خطر در خارج از دنیای فضای سایبر هم وجود دارد. بنابراین تفاوت بیشتر در درجه است تا نوع. دیگران این رویکرد ظاهرگرا را رد می کنند و استدلال آن ها اینست که برای ارزیابی زمان به راه انداختن ماده ۵۱ ضابطه میزان و اثرات دیوان کارآمدتر است. این نظر با دیدگاه دیوان مبنی بر این که بین توسل به زور و حمله مسلحانه تفاوت ماهوی است، موافق است. دیوان بین المللی دادگستری برای تمایز ما بین شدیدترین اشکال توسل به زور من جمله حمله مسلحانه و اشکال با شدت کمتر ضابطه « میزان و اثر» را اعمال کرده است.ICJ Reports,op.cit.,(1986),para. 191,103 para.195 . .. پروتکل اول الحاقی به کنوانسیون ۱۹۴۹ ژنو، حمله را عمل خشونت آمیز علیه دشمن تعریف می کند. بنابراین حمله مسلحانه، یک عمل یا یک دسته از عملیات نظامی مسلحانه است که هم شدت قابل توجهی داشته و هم نتایج آن تخریب و نابودی اساسی عناصر حیاتی دولت قربانی از جمله، ساختارهای اقتصادی و امنیتی، از بین بردن اقتدار دولتی و استقلال سیاسی و همچنین قربانی کردن مردم و محروم ساختن دولت از دارایی های فیزیکی همچون قلمرو ش است(International Law and Article 51 of the UN Charter",(2000),63-64 باید اشاره کرد که تجهیزات سایبری می تواند سلاح و کاربرد آن ها تحت شرایطی حمله مسلحانه محسوب شود. مسلحانه محسوب شود. بنابراین، دیدگاه غالب بین کارشناسان حقوقی، برای تعیین این که آیا یک حمله سایبری به حد حمله مسلحانه می رسد یا نه، اینست که بر نتایج حوادث تکیه کرده و بر تحلیلی تأثیرگرایانه را از یک حمله سایبری تأکید دارند، در حالی که حمله سایبری اتفاقی بوده یا هدف واقعاً دولت دیگری باشد، اما اتفاقاً موجب ورود صدمه به دوتتی دیگر شود(.International Law op. Cit.,p. 902).
معلوم نیست که دولت قربانی واقعاً حق توسل به دفاع مشروع را دارد یا نه. نظر دیوان در قضیه سکوهای نفتی بر این بود که حمله مسلحانه می بایست با قصد معین وارد آوردن صدمه باشد (ICJ Reports 2003, 161 et seq. 191.para.64) .

قابلیت انتساب حمله سایبری به دولت

انتساب یک حمله سایبری به یک دولت، عنصر کلیدی در ساخت یک رژیم حقوق کارا در کاهش این نوع حملات است. در حوزه قواعد حاکم بر مسئولیت بین المللی دولت ها همیشه یکی از سوالات کلیدی اینست که آیا اعمال انجام شده از طرف افراد و گروه ها به دولت ها منسوب می شود تا در نتیجه مسئولیت بین المللی دولت ها به وجود آید. از آنجایی که در حقوق بین الملل برای آن که عملی به لحاظ بین المللی متخلفانه محسوب می گردد، حتماً باید به یک دولت منتسب شود و از سوی دیگر دولت به عنوان یک شخص انتزاعی نمی تواند تصمیم گیری و عمل نماید، از طریق اشخاص حقیقی این کار را انجام می دهد (Juridical International, Nbr. XI, January 2006. p. 187.) . پس در واقع این مأموران و نمایندگان دولت هستند که مرتکب اعمال متخلفانه می شود و زمینه مسئولیت بین-المللی دولت را فراهم می آورند. بدین ترتیب مطابق آن چه که به موجب دکترین، عرف، رویه قضایی و طرح کمیسیون حقوق بین الملل در خصوص مسئولیت بین المللی دولت ها آمده است، قاعده کلی انتساب اعمال متخلفانه به دولت ها اینست که صرفاً اعمالی که توسط ارگان های یک دولت یا اعمالی که با هدایت، تحریک یا کنترل او انجام گرفته قابل انتساب به دولت است (Cyber Warfare and Cyber terrorism, 2008, Information science reference,p. 98.) از این عبارت بر می آید که اصولاً حقوق حاکم بر مسئولیت دولت مبتنی بر نظریه نمایندگی است. پس در راستای انتساب مسئولیت یک رفتار متخلفانه که بین¬المللی به دولت می بایست تعیین سازیم که آیا شخص در ارتکاب آن رفتار به نمایندگی از یک اعمال دولت محسوب می شود. نتیجه منطقی قاعده انتساب و اصل حاکم بر مسئولیت بین المللی دولت ها این است که رفتار و اعمال ارگان-های خصوصی ـ چه اشخاص چه نهادها ـ به خودی خود قابل انتساب به دولت نیست، مگر آن که مطابق ماده ۸ طرح مسئولیت بین المللی دولت ها، فرد یا افراد خصوصی به دستور ، هدایت و یا به طور کلی تحت کنترل آن دولت دست به رفتار متخلفانه زده باشند. با این حال تعریف دقیق کنترل و حدود آن مشخص نشده و تفسیر این امر به دادگاه ها واگذار شده است . بطور خلاصه باید اشاره داشت که تاکنون دو ضابطه در خصوص نحوه انتساب رفتار ارگان های غیردولتی به دولت ها توسط رویه قضایی بین المللی مورد شناسایی واقع شده است. این دو مورد عبارتند از: کنترل موثر Effective controlو کنترل کلی Overal control از سوی دیگر جدای از مباحث پیرامون کنترل دولت، در باب مسئولیت دولت از بابت اعمال افراد خصوصی عنوان شده که مسئولیت دولت نه تنها می تواند برخاسته از فعل او باشد بلکه ناشی از ترک فعلش هم می تواند باشد. بنابراین دولتی که از وظیفه پیشگیری از این که فعالیت های انجام شده در سرزمینش موجب ورود صدمه به دولت دیگر نشود، تخلف کرده و کوشش مقتضی را در این میسر به کار نسته مسئول نقض تعهدات خویش است.

حمله سایبری دولتی

مواد کمیسیون حقوق بین الملل در خصوص مسئولیت دولت بر این اصل حقوقی استوار شده که برای انتساب مسئولیت به دولت، ارگانی که عمل متخلفانه را انجام می دهد باید یک نهاد دولتی باشد بنابراین قبل از آن که دولت بابت اعمال انجام شده از داخل قلمروش مسئول تلقی شود باید مسئولیت نیابتی اش ثابت شود.

دفاع مشروع در مقابل حمله سایبری

ماده ۵۱ منشور سازمان ملل متحد مقرر می دارد: « در صورت حمله مسلحانه علیه یک عضو سازمان ملل متحد، تا زمانی که شورای امنیت اقدامات لازم را برای حفظ صلح و امنیت بین المللی به عمل آورد، هیچ یک از این منشور به حق دفاع مشروع انفرادی یا دسته جمعی اعضا لطمه ای وارد نخواهد کرد اعضا باید اقداماتی را که در اعمال این حق دفاع از خود، به عمل می آورند، فوری به شورای امنیت گزارش دهند. این اقدامات به هیچ وجه در اختیار و مسوولیتی که شورای امنیت طبق این منشور دارد و به موجب آن برای حفظ و اعاده صلح و امنیت بین المللی در هر موقع که ضروری تشخیص دهد اقدام لازم را به عمل خواهد آورد، تأثیری نخواهد داشت.

نتیجه گیری

درعصر حاضرشاید دولتهادیگر کمترازابزار نظامی برای نشان دادن قدرت خود استفاده کنند.چون راههای دیگری نیز برای اعمال قدرت وجوددارد ازجمله حملات سایبری که به طور تفصیلی به آن اشاره کردیم که درحقیقت امر حملات سایبری خود به گونه ای فشار بین المللی محسوب می شود .اما ذکراین مطلب نیز ضروری به نظر می رسد که با تمام این تفاسیر دولتها در حملات سایبری تا جایی که ممکن است سعی می کنند انتساب خود را به این موارد نفی کنند تا منافعشان به خطر نیفتد . مسئولیت بین¬المللی دولت در قبال حمله سایبری در درجه اول منوط به توصیف آن به عنوان عمل متخلفانه بین¬المللی و در درجه بعد انتساب آن به یک دولت مشخص است. در تبیین وضعیت دولت¬های زیان دیده از حملات سایبری نیز باید گفت که چنانچه این حملات در تناقض با تعهدات جمعی دولت¬ها یا به عبارت در دیگر در تعارض با منافع جامعه جهانی باشد، سایر دولت¬ها غیر از دولت قربانی نیز محق به طرح دعوای مسئولیت دولت پشتیبان حمله می-شوند. ازآنجایی که فضای سایبری این امکان رافراهم می کندکه اشخاص حقوقی هم به حمله سایبری اقدام کنندحملات افراددراین صورت زمانی منتسب به دولت خواهد بودکه این افراد تحت استخدام وهدایت دولت باشند .دراین حالت باید بین مقصر ومرتکب قائل به تفکیک وبررسی بود که خود روندی پیچیده در پی خواهدداشت.

فهرست منابع

۱. امیر حسین، جلالی فراهانی، تروریسم سایبری، نشریه فقه و حقوق، شماره ۱۰، ۱۳۸۵

۲. یاسر ضیایی، حمایت از حقوق بشر در فضای سایبر، مجله پژوهشهای حقوقی، شماره ۲۱، ۱۳۹۲.

۳. سید قاسم زمانی و سید یاسر ضیایی، تعمیم نظام مسئولیت بین‌المللی به بازیگران غیردولتی؛با تأکید بر مسئولیت بین‌المللی جدایی‌طلبان، مجله حقوقی بین‌المللی، شماره ۴۵، ۱۳۹۱

۴. سازمان ملل، نشریه بین المللی سیاست جنائی، ترجمه دبیرخانهٔ شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور، ۱۳۷۶

۵. علیرضا ابراهیم گل، متن و شرح مواد کمیسیون حقوق بین‌الملل در خصوص مسؤولیت بین‌المللی دولت، نشر شهر دانش، ۱۳۸۸.

۶. علیرضا انتظاری و سید مصطفی محقق داماد، نقش اتلاف و تسبیب در مسؤولیت مدنی زیست محیطی، مجله مطالعات اسلامی، شماره ۸۹، ۱۳۹۱.

منابع لاتین

7 . Draft articles on Responsibility of States for Internationally wrongful Acts (2001)

8 . Factory of Chorzow, Merits, 1928,P.C.I.J, Series A No.17, p.47

9.Rex B. Hughes, NATO and Cyber Defence: Mission Accomplished?, ATLANTISCH PERSPECTIEF (Apr. 2009), available at http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf

10.The Central Intelligence Agency (CIA) is an independent US Government agency responsible for providing national security intelligence to senior US policymakers.

11.The National Aeronautics and Space Administration (NASA) is the agency of the United States government that is responsible for the nation's civilian space program and for aeronautics and aerospace research. http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

12. http://www.au.af.mil/au/awc/awcgate/army/jaoac-io.pdf U.S. Department of Defense Report.

13. A/RES/36/103, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States 91st plenary meeting, 9 December 1981.

14.Putin Warns Against Belittling War Effort, Radio Free Europe, May 9, 2007. Available at: http://www.rferl.org/featuresarticle/2007/05/704c2d80-9c47-4151-ab76-

15.Declaration on the Inadmissibility of Intervetion into Domestic Affairs of States and Protection of Their Independence and Sovereignty, G.A. RES. 2131, 20 th Sess., Supp. No. 14

16.Draft Articles on the Responsibility of States for Internationaly Wrongful Acts Adopted by International Law Commission of United Nation Organization.

17.Draft Artcles on Prevention of Transboundary Harm from Hazardous activities,Adopted by Internatinal Law Commission of United Nation,2001.

18.Draft Principle on the Allocation of Loss in the case of transboundary harm arising out of hazardous activities, Yearbook of International Law Commission (/ /1/10), vol. II.

19.Directive 2004/35/CE of the European Parliament and of the Council of 21 April 2004 on Environment liability with regard to Prevention and Remedying of Environment Damage, Official Journal of European union

20.National Research Committee on Offensive Information Warfare, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber-Attacks Capabilities (NRC Committee Report),(2001), Available at:
http://www.safeguardingaustraliasummit.org.au/uploader/resources/d uncan _ unwin.pdf.

21.G.A.Res3314,U.N.DOC.A/RES/3314 (Dec,14,1974) .Available at: http://www.daccess-ddsny.un.org/doc/resolution/gen/nro/739/16/nro73916.pdf>

22.“National Military Strategy for Cyber Operation”, Department of Defense Cyber Space Policy Report, November 2011, Section 3.

23.ICC Assembly of State Parties, Special working group on the Crime of aggression Second Resump. 7 th Sess., New York, Feb. 9-13 2009, Report of the Special working group on the Crime of Aggression, Annex II. Annex. I. ICC-ASP/7/20/Add.1(SWGCA).

24.Resloution adopted by G.A. 6.January 2006 on the Report of the sixth Committee (A169/519).

25.Vienna Convention on Civil liability for Nuclear Damage,1963, U.N. Treaty Series, Vol. 1063,p. 265.

26. Vienna Convention on the law of Treaties, 1966.